UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

FRED WHELAN JR., on behalf of himself and all others similarly situated, Plaintiff, v. DILIGENT CORPORATION, Defendant.	Case No. 22-cv-7598 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, Fred Whelan Jr. through his attorneys, bring this Class Action Complaint against the Defendant, Diligent Corporation ("Diligent" or "Defendant"), alleging as follows:

INTRODUCTION

1. Diligent, a software-as-a-service company serving corporate boards across the country, lost control over its employees' highly sensitive personal information in a May 2022 data breach by cybercriminals ("Data Breach").

2. On or around May 21, 2022, hackers bypassed Diligent's cybersecurity safeguards undetected and breached its systems. On information and belief, once inside, cybercriminals were able to pilfer the personally identifiable information ("PII") belonging to over 1,100 Diligent employees.

3. That PII included employees' human resources records, such as their names, email addresses, mailing addresses, and Social Security numbers.

4. Diligent's "security team" did not discover the hack until two days later, meaning Diligent had no effective means to prevent, detect, or stop data breaches before cybercriminals

could access employee PII.

5. Diligent is well-aware of its duty to protect sensitive information. As part of its services, it grades its clients on their cybersecurity preparedness, assigning them a "Cyber Risk Scorecard" that "highlight[s] cybersecurity vulnerabilities and help prevent data breaches."[1]

6. Diligent also promises to "implement technical and organizational measures to ensure a level of security appropriate to the risk to the personal information we process."[2] In other words, Diligent acknowledges it has a duty to protect PII using reasonable means commensurate with the highly sensitive data it collects.

7. Indeed, Diligent has a duty to protect employee PII through its policies and state and federal law.

8. On information and belief, Diligent failed in that duty because it did not implement or adhere to cybersecurity measures that would have prevented or stopped cybercriminals from accessing its employees' PII.

9. Following the Data Breach, Diligent said that it would "further enhance its security controls, including by migrating additional workloads and data to the Diligent-managed environment[,]"—security measures that it should have implemented *before* the Data Breach.

10. Diligent's negligent conduct puts Plaintiff and Diligent's current and former employees at risk.

11. Armed with the employees' PII, data thieves can commit various crimes including, e.g., opening new financial accounts in employees' names, taking out loans in

[1] *See* SecurityScorecard's website article announcing its partnership with Diligent at https://securityscorecard.com/company/press/diligent-delivers-cyber-risk-scores-directly-to-board-directors (last visited Aug. 8, 2022).

[2] *See* Diligent's privacy policy at https://www.diligent.com/privacy/ (last visited Aug. 8, 2022).

employees' names, using employees' names to obtain medical services, using employees' information to obtain government benefits, filing fraudulent tax returns using employees' information, obtaining driver's licenses in employees' names but with another person's photograph, and giving false information to police during an arrest.

12. As a result of the Data Breach, Diligent's current and former employees have been exposed to a heightened and imminent risk of fraud and identity theft. They must now and in the future closely monitor their financial accounts to guard against identity theft.

13. Employees also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

14. By their Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose PII was accessed during the Data Breach.

15. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Diligent's data security systems, future annual audits, and adequate credit monitoring services funded by Diligent.

PARTIES

16. Plaintiff, Fred Whelan, is a natural person and citizen of Massachusetts, residing in Massachusetts, where he intends to remain. Plaintiff Whelan is a former Diligent employee and Data Breach victim, receiving Diligent's Breach Notice in June 2022. Plaintiff Whelan worked for Diligent from approximately 2015 to 2016.

17. Defendant, Diligent, is a New York Corporation, with its principal place of business at 111 W 33rd St 16th Floor, New York, NY 10001.

JURISDICTION & VENUE

18. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

19. This Court has personal jurisdiction over Defendant because Diligent maintains its principal place of business in this District and does substantial business in this District.

20. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

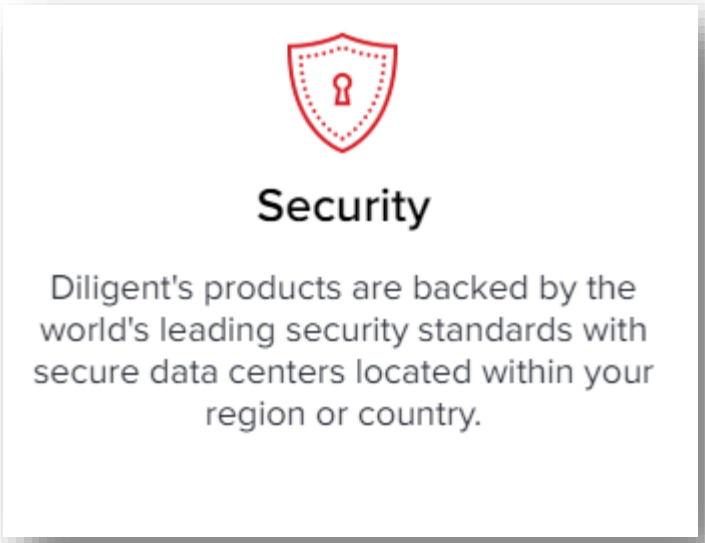
BACKGROUND FACTS

a. Diligent

21. Diligent is a "SaaS" company that provides management software to corporate boards. Holding itself out as the "#1 Global Board Meeting Software," Diligent says that "Diligent Board Management Software fulfills the board's ability to meet the challenges of modern governance by providing your board with the right tools, analytics and insights to get a better pulse on the market and overall performance of your business."[3]

22. In so doing, Diligent advertises that it employs the "world's leading security standards" to protect information stored on its systems:

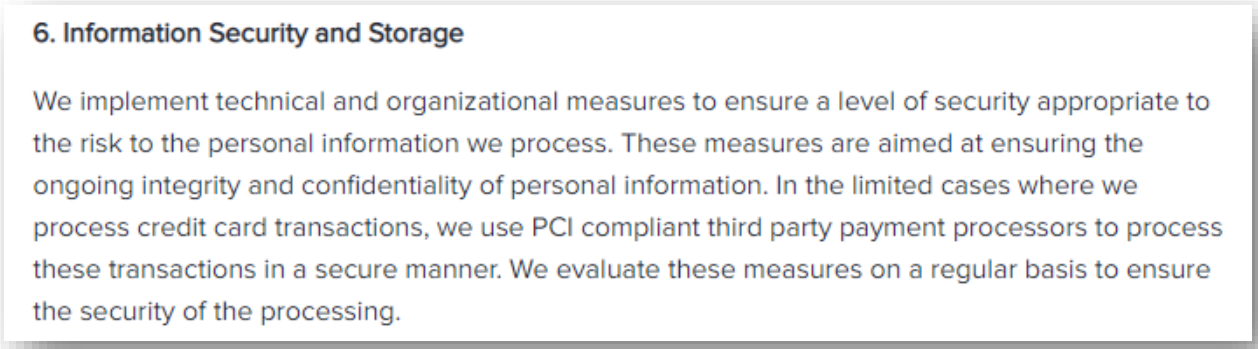
[3] *See* Diligent's landing page at https://www.diligent.com/landing/solutions/lp-board-portal-demo/?&utm_source=google&utm_medium=cpc&_bt=611705541966&_bk=diligent%20corporation&_bm=b&_bn=g&gclid=CjwKCAjw6MKXBhA5EiwANWLODLEKe17KlKrUU0AwTofmfF135LImmeZWupSe_KQ2sCTJRh4ScR-0MRoCCOUQAvD_BwE&gclsrc=aw.ds (last visited Aug. 8, 2022).



4

23. It also consults on cybersecurity for its clients using cybersecurity "scorecards" that grade a company's security systems.[5]

24. Diligent's privacy policy promises to protect the sensitive information it collects using "a level of security appropriate to the risk to the personal information we process."[6]



[4] *Id.*

[5] *See* SecurityScorecard's website article announcing its partnership with Diligent at https://securityscorecard.com/company/press/diligent-delivers-cyber-risk-scores-directly-to-board-directors (last visited Aug. 8, 2022).

[6] *See* Diligent's privacy policy at https://www.diligent.com/privacy/ (last visited Aug. 8, 2022).

25. But, on information and belief, Diligent fails to strictly adhere to these policies in maintaining its own employees' PII.

b. Diligent Fails to Safeguard Employee PII

26. Plaintiff Whelan is a former employee of Diligent.

27. As a condition of employment with Diligent, employees were required to disclose their PII, including names, email addresses, mailing addresses, and Social Security numbers.

28. Diligent collects and maintains that employee PII in its computer systems, even after employees no longer worked for Diligent.

29. In collecting and maintaining the PII, Diligent agreed it would safeguard the data according to its internal policies and state and federal law.

30. Even so, on or about May 21, 2022, hackers bypassed Diligent's security systems and accessed employee PII.

31. Hackers did so undetected, as Diligent would not discover the hack until two days after it started.

32. By the time Diligent's "security team" discovered the Data Breach, cybercriminals had already accessed its employees' PII, including their names, email addresses, mailing addresses, and Social Security numbers.

33. After discovering the breach, Diligent claims that it "contained the event" the next day.

34. Diligent then "investigate[d]" the breach and notified its employees about the breach one month later. A true and correct copy of the breach notice ("Breach Notice") is attached as **Exhibit A**.

35. Although Diligent investigated the Data Breach for a month before notifying its

employees, Diligent's Breach Notice did not explain how the hack happened, why it took three days for Diligent to detect and contain the hack, exactly what information the hackers stole from individuals, whether Diligent paid a ransom to the hackers, and whether it knows if its employees' information was shared on the dark web. Indeed, Diligent disclosed that employees' information only "may have been accessed" without clarifying exactly what information hackers accessed.

36. On information and belief, cybercriminals could breach Diligent's systems because Diligent failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over employee PII. Diligent's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PII. Further, the Breach Notice makes clear that Diligent cannot, or will not, determine the full scope of the Data Breach, as it has been unable to determine exactly what information was stolen and when.

37. On information and belief, a ransomware hacker group named HiveLeaks were the cybercriminals that breached Diligent's systems.

38. On information and belief, HiveLeak routinely posts stolen PII on the dark web following data breaches.

c. Plaintiff Whelan's Experience

39. Plaintiff is a former Diligent employee.

40. As a condition of Plaintiff's employment, Diligent required him to provide his PII.

41. Plaintiff provided his PII to Diligent and trusted that the company would use reasonable measures to protect it according to Diligent's internal policies and state and federal

law.

42. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

43. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff fears for his personal financial security and uncertainty over what Private Information was exposed in the Data Breach. He is also receiving spam calls and texts following the Data Breach, showing that his information is being misused to persistently contact him with unwanted solicitations.

44. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

45. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

46. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

47. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

d. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

48. Plaintiff and members of the proposed Classes have suffered injury from the misuse of their PII that can be directly traced to Defendant.

49. As a result of Diligent's failure to prevent the Data Breach, Plaintiff and the proposed Classes have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PII in their possession.

50. Stolen PII is one of the most valuable commodities on the criminal information

black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

51. The value of Plaintiff and the proposed Classes' PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

52. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

53. One such example of criminals using PII for profit is the development of "Fullz" packages.

54. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

55. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Classes' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Classes, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Classes' stolen PII is being misused, and that

such misuse is fairly traceable to the Data Breach.

56. Defendant disclosed the PII of Plaintiff and members of the proposed Classes for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and members of the proposed Classes to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

57. Defendant's failure to properly notify Plaintiff and members of the proposed Classes of the Data Breach exacerbated Plaintiff and members of the proposed Classes' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

e. Defendant failed to adhere to FTC guidelines.

58. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

59. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

60. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

61. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

62. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

63. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

CLASS ACTION ALLEGATIONS

64. Plaintiff sues on behalf of himself and the proposed nationwide class ("Class") and state subclass ("Subclass") (together "Classes"), defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

> **Nationwide Class**: All individuals residing in the United States whose PII was compromised in the Data Breach.
>
> **Massachusetts Subclass**: All individuals residing in Massachusetts whose PII was

compromised in the Data Breach.

Excluded from the Classes are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

65. Plaintiff reserves the right to amend the class definition.

66. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is representatives of the proposed Classes, consisting of at least 1,100 members, far too many to join in a single action;

b. **Ascertainability**. Members of the Classes are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Classes' interests. Their interests do not conflict with the Classes' interests and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Classes' behalf, including as lead counsel.

e. **Commonality**. Plaintiff and the Classes' claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Classes. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff and the Classes' PII;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PII;

iv. Whether Defendant breached contract promises to safeguard Plaintiff and the Classes' PII;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff and the Classes' injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Classes are entitled to damages, treble damages, or injunctive relief.

67. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Classes)

68. Plaintiff realleges all previous paragraphs as if fully set forth below.

69. Plaintiff and members of the Classes entrusted their PII to Defendant. Defendant owed to Plaintiff and other members of the Classes a duty to exercise reasonable care in handling

and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

70. Defendant owed a duty of care to Plaintiff and members of the Classes because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff and members of the Classes' PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

71. Defendant owed to Plaintiff and members of the Classes a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Classes the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Classes to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

72. Defendant owed these duties to Plaintiff and members of the Classes because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff and members of the Classes' personal information and PII.

73. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

74. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and members of the Classes' and the importance of exercising reasonable care in handling it.

75. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and members of the Classes which actually and proximately caused the Data Breach and Plaintiff and members of the Classes' injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Classes, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and members of the Classes' injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Classes have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

76. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Classes actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are

ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence Per Se
(On Behalf of Plaintiffs and the Classes)

77. Plaintiff and members of the Classes incorporate the above allegations as if fully set forth herein.

78. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and members of the Classes' PII.

79. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the members of the Classes' sensitive PII.

80. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its employees' PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its employees in the event of a breach, which ultimately came to pass.

81. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and

deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Classes.

82. Defendant had a duty to Plaintiff and the members of the Classes to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Classes' PII.

83. Defendant breached its respective duties to Plaintiff and members of the Classes under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Classes' PII.

84. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

85. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Classes, Plaintiff and members of the Classes would not have been injured.

86. The injury and harm suffered by Plaintiff and members of the Classes were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Classes to suffer the foreseeable harms associated with the exposure of their PII.

87. Had Plaintiff and members of the Classes known that Defendant did not adequately protect their PII, Plaintiff and members of the Classes would not have entrusted Defendant with their PII.

88. As a direct and proximate result of Defendant's negligence per se, Plaintiff and members of the Classes have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft;

lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III
Breach of an Implied Contract
(On Behalf of Plaintiff and the Classes)

89. Plaintiff and members of the Classes incorporate the above allegations as if fully set forth herein.

90. Defendant offered to employ Plaintiff and members of the Classes in exchange for their PII.

91. In turn, and through internal policies, Defendant agreed it would not disclose the PII it collects to unauthorized persons. Defendant also promised to safeguard employee PII.

92. Plaintiff and the members of the Classes accepted Defendant's offer by providing PII to Defendant in exchange for employment with Defendant.

93. Implicit in the parties' agreement was that Defendant would provide Plaintiff and members of the Classes with prompt and adequate notice of all unauthorized access and/or theft of their PII.

94. Plaintiff and the members of the Classes would not have entrusted their PII to Defendant in the absence of such agreement with Defendant.

95. Defendant materially breached the contract(s) it had entered with Plaintiff and members of the Classes by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information.

Defendant further breached the implied contracts with Plaintiff and members of the Classes by:

a. Failing to properly safeguard and protect Plaintiff and members of the Classes' PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

96. The damages sustained by Plaintiff and members of the Classes as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

97. Plaintiff and members of the Classes have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

98. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

99. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

100. Defendant failed to advise Plaintiff and members of the Classes of the Data Breach promptly and sufficiently.

101. In these and other ways, Defendant violated its duty of good faith and fair dealing.

102. Plaintiff and members of the Classes have sustained damages because of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Classes)

103. Plaintiff and members of the Classes incorporate the above allegations as if fully set forth herein.

104. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

105. Plaintiff and members of the Classes conferred a benefit upon Defendant in the form of services through employment.

106. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Classes. Defendant also benefited from the receipt of Plaintiff and members of the Classes' PII, as this was used to facilitate their employment.

107. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the proposed Classes' services and their PII because Defendant failed to adequately protect their PII. Plaintiff and the proposed Classes would not have provided their PII or worked for Defendant at the payrates they did had they known Defendant would not adequately protect their PII.

108. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Classes all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

COUNT V
Invasion of Privacy, Mass. Gen. Laws. Ch. 214 § 1B
(On Behalf of Plaintiff Whelan and the Massachusetts Subclass)

109. Plaintiff and members of the Subclass incorporate all previous paragraphs as if fully set forth herein.

110. Plaintiffs and the Subclass had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

111. Defendant owed a duty to its patients, including Plaintiff and the Subclass, to keep this information confidential.

112. The unauthorized acquisition (*i.e.,* theft) by a third party of Plaintiff and Subclass members' PII is highly offensive to a reasonable person.

113. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Subclass disclosed their sensitive and confidential information to Defendant to receive pharmaceutical services, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Subclass were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

114. The Data Breach constitutes an intentional interference with Plaintiff and the Subclass's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

115. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

116. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Subclass in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

117. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Subclass.

118. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Subclass were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Subclass to suffer damages.

119. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Subclass since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

120. Plaintiff and the Subclass have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Subclass.

121. In addition to injunctive relief, Plaintiff, on behalf of himself and the other members of the Subclass, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT VI
Declaratory Judgment and Injunctive Relief
(On behalf of Plaintiff and the Classes)

122. Plaintiff incorporate all previous paragraphs as if fully set forth below.

123. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious and which violate the terms of the federal and state statutes described above.

124. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiff allege Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Classes continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

125. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed, and continues to owe, a legal duty to employ reasonable data security to secure the PII with which it is entrusted, specifically including information pertaining to financial records it obtains from its employees, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

b. Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

c. Defendant's breach of its legal duty continues to cause harm to Plaintiff and the Classes.

126. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its employees' (i.e. Plaintiff and the Classes') data.

127. If an injunction is not issued, Plaintiff and the Classes will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiff and the Classes will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Classes for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Classes, which include monetary damages that are not legally quantifiable or provable.

128. The hardship to Plaintiff and the Classes if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued.

129. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Classes, and the public at large.

PRAYER FOR RELIEF

Plaintiff and members of the Classes demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Classes, appointing Plaintiff as class representatives, and appointing their counsel to represent the Classes;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Classes;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Classes;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Classes damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Classes in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Classes leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

RESPECTFULLY SUBMITTED AND DATED this 6th day of September, 2022.

/s/ James J. Bilsborrow
James J. Bilsborrow
WEITZ & LUXENBERG, PC
700 Broadway
New York, NY 10003
T: (212) 558-5500
F: (212) 344-5461
jbilsborrow@weitzlux.com

Samuel J. Strauss (*pro hac vice* forthcoming)
Raina C. Borrelli (*pro hac vice* forthcoming)
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
T: (608) 237-1775
F: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

Attorneys for Plaintiff